Testimony of Erich Spengler
Director/PI, NSF ATE Regional Center for Systems Security and Information Assurance (CSSIA)
Associate Professor, Computer Integrated Technology, Moraine Valley Community College

July 21, 2004

Good morning, Mr. Chairman and Members of the Committee. I would like to thank the Committee for the opportunity to comment on the role of community colleges in cybersecurity education. My name is Erich Spengler, and I am the Director and Principal Investigator for the National Science Foundation's ATE Regional Center for Systems Security and Information Assurance (CSSIA). I come to you with 16 years of combined experience in the classroom and the IT Industry. I am currently an Associate Professor in Computer Integrated Technology at Moraine Valley Community College in Palos Hills, Illinois.

- **What roles do community colleges play in the training of new workers and the retraining of current workers? What employment opportunities in cybersecurity are available for individuals with a certificate or a two-year degree?**

Role of Community Colleges

Community colleges play a critical role in the education and training the Nation's workforce. Some 1,173 community and technical colleges enroll 44% of all U.S. undergraduate students. The American Association of Community Colleges (AACC) notes that 200,000 certificates and 450,000 associate's degrees are granted each year. With an enrollment of 5.4 million credit students and 5 million non-credit students, these institutions train and educate a significant percentage of the workforce.

One of the strengths of community colleges is the close relationship they maintain with local business and industry. This relationship may take many forms. For example, community college faculty are often asked to develop and deliver customized training solutions for business partners. Business partners play an important role in shaping career and technical programs by their participation as members of advisory committees. Another strength is the flexibility of the community college curriculum, which is often designed specifically to train practitioners. This flexibility enables community colleges to respond quickly to changes in technology. Community colleges also establish career pathways from high schools to two-year career programs and then additional pathways to four-year colleges or universities. This articulation of curriculum allows students to seamlessly continue higher levels of professional studies and education close to home.

Employment Opportunities

The NSF ATE Regional Center for Systems Security and Information Assurance (CSSIA) and its partners recently conducted a survey (http://www.cssia.org) of companies in five mid-western states to determine the job demand for IT security-related positions, desired skills, and preferred educational levels. I would like to share some of those results at this time.

- A total of 340 responses were received. Respondents were divided into small (less than 100 employees), medium (100-499) and large (500 or more) companies.
- An overwhelming 99% of respondents were concerned about Internet and computer security.
- Almost three-fourths of respondents said their company currently employed people in IT security positions.

- IT security positions were more likely to be part-time or shared positions (part-time security along with other IT duties) than dedicated (full-time IT security).

Table 1
Present/Projected Employment Needs for IT Security Positions

	Number Responding	Number of Openings	
		Dedicated Responsibility	Added Responsibility
Number of present openings	53	63	103
Number of projected openings within one year	60	96	141
Number of projected openings within three years	60	164	258

- Security responsibilities are being added to most IT professions, including network administrators, help desk specialists, network engineers, application developers, and systems analysts.
- Slightly more than half said there was a shortage in the current supply of qualified applicants for entry-level IT security positions.
- Large companies were more likely to be concerned about Internet and computer security and to have dedicated security positions.
- The most popular types of security training were self-study, commercial vendor training sites, and community college programs.

Table 2
Required Educational Level For An
Entry-Level IT Security Position
N = 241

	Minimum	Preferred
None	7%	2%
High school diploma or GED	14%	1%
Certificate/licensure	15%	15%
Associate's degree	24%	13%
Bachelor's degree or higher	31%	62%
Other	9%	8%

- There are significant opportunities for individuals who possess an Associate's degree.
- Respondents indicated a significant number of current open IT security positions and projected even more openings over the next three years.

Community colleges must continue to respond to growing industry demands for professionals possessing cybersecurity skills. Although it is clear that there are career opportunities for professionals holding Associate's degrees, we must continue to develop pathways with four-year colleges and universities allowing those professionals to attain a higher level of education.

- **What are the current strengths and weaknesses of cybersecurity education and training programs? What "model" courses and programs currently exist? And what types of courses or programs need to be developed or more broadly implemented?**

Current strengths and weaknesses of cybersecurity education and training programs

Current strengths of cybersecurity education include the utilization of NSF ATE centers as resources for faculty development, internship programs and processes, dissemination and implementation of curriculum models, collaboration, and partnerships among academic institutions and business and industry. In addition, opportunities exist for community college faculty to participate in cybersecurity initiatives and information sharing with government-sponsored groups such as the FBI's InfraGard and the United States Secret Service Electronic Crimes Task Force.

However, much of the current cybersecurity curriculum typically focuses on networking-related technologies. There is a need to expand the emphasis beyond networking to serve the greater spectrum of IT curriculum. Specialties might included forensics, programming and secure coding, information assurance, and e-commerce and secure communications.

Community colleges are also challenged to integrate security-related coursework into existing IT programs and degrees. Three career areas must be addressed: (1) the focused cybersecurity practitioner specializing in their field of study, (2) the IT professional not dedicated to security but who is charged with the protection of critical information and infrastructure, and (3) non-IT-related professionals such as healthcare personnel.

Model courses and programs

As cybersecurity technology emerges so must the programs within the community colleges. There is debate regarding modeling of curriculum on industry certification. This debate centers on the delicate balance between certification preparation and required skill sets. Certifications provide a reasonable direction and solid groundwork representing industry needs. However, barriers exist for standardized academic models that reflect the skills defined by these industry certifications: (1) security-related industry certifications continue to proliferate, making it difficult to identify which certifications would provide the best models, and (2) skills outlined in industry certification often require costly effort to be implemented into an academic framework.

Community colleges have identified four approaches to developing and offering courses and programs: (1) four-semester programs of study leading to Associate's degrees, (2) two-semester programs leading to institution-conferred certificates, (3) credit courses that are part of an existing program of study, and (4) non-credit programs of preparation for industry certification.

The NSF ATE Regional Center for Systems Security and Information Assurance (CSSIA) is developing an adoptable model that reflects both industry certifications and practitioners' required skills. The CSSIA center is working within each of the partner states to establish model four-semester and certificate programs that reflect current and relevant industry certifications and skills.

Development of programs

Collaboration among community colleges to reduce duplication of efforts is still needed. The establishment of cybersecurity programs can be expensive and require a prolonged development cycle. Additionally, we should consider the importance of the adaptation and dissemination of instructional materials and best practices. As an example, to help reduce implementation costs of quality learning environments, the NSF ATE CSSIA center developed an innovative use of laboratory equipment through remote access and management. Additionally, partnering with national program models, such as the Cisco Systems Networking Academy, allows for greater implementation and consistency of curriculum.

- **What are the challenges you face in recruiting and training cybersecurity faculty? What type of programs or opportunities do you provide to help keep faculty current?**

Challenges in recruiting and training cybersecurity faculty

The greatest challenge facing community colleges and their efforts to establish cybersecurity programs is faculty recruitment and development. Community colleges must try to compete with business and industry for skilled practitioners. An additional challenge occurs when individuals interested in becoming faculty members possess the necessary technological skills, but lack teaching experience.

Programs or opportunities to help keep faculty current

In 2002, the American Association of Community Colleges (AACC) sponsored the AACC/NSF Cybersecurity Workshop. The workshop served as a catalyst for community college professionals interested in cybersecurity by identifying workforce and curricular needs and by establishing a forum for collaboration among community colleges.

The NSF ATE program has provided vital resources to a number of community colleges in an effort to establish cybersecurity programs. These projects allocate a significant portion of the funding for faculty development. The funds can be used in activities such as product training, professional externship opportunities, and graduate-level courses and workshops.

During the summer of 2004, the NSF ATE Regional Center for Systems Security and Information Assurance (CSSIA) trained over 200 college faculty in Security Awareness, Information Assurance, Network Security, and Wireless technologies. CSSIA will continue to provide training opportunities in new and emerging skills for faculty in subsequent years. It is clearly our belief that without these training programs, the cybersecurity initiatives available to attending faculty would not move forward to meet growing industry practitioner demands. Another model designed to keep faculty current in emerging IT skills is the Working Connections Faculty Development Institute. Working Connections is co-sponsored by the NSF ATE National Workforce Center for Emerging Technologies (NWCET), AACC and Microsoft Corporation to develop professional skills of faculty in several regions throughout the US.

- **What can the federal government do to improve cybersecurity education and build the Nation's technical workforce?**

First, the federal government can encourage government agencies to provide to community colleges their job descriptions and titles that are appropriate for cybersecurity graduates of two-year community and technical college programs.

Next, to improve cybersecurity education and build the Nation's technical workforce, the federal government must continue to invest in the programs and people that are making a difference in the education and training of our cybersecurity workforce. Without the support from programs such as the NSF Advanced Technological Education (ATE) Program, many institutions would not have the resources or faculty expertise to meet the challenges required to build quality cybersecurity programs.

This concludes my statement Mr. Chairman and members of the committee. Thank you for allowing me to address the committee on this issue.

Biographical Information

Erich J. Spengler, M.B.A.
Director/PI - CSSIA
NSF Regional Center for Systems Security and Information Assurance

Erich Spengler holds a Master's degree from Loyola University and has been a full-time faculty member at Moraine Valley Community College for the past nine years. Mr. Spengler also has an extensive background in information technology, security and information assurance. He holds several major industry certifications, including CISSP, MCSE and CCNP. Additionally, he has a broad background in network design and infrastructure implementation.

Mr. Spengler currently serves as the Director and Principle Investigator for the National Science Foundation (NSF) ATE Regional Center for Systems Security and Information Assurance (CSSIA). This regional center serves a five-state area of the Midwest and focuses on a field which is critical to homeland security and which has a large demand for qualified workers. The center is collecting, adapting, and enhancing curricula in cybersecurity, modeling certificate and degree programs, and providing professional development for college faculty in the region.